NOTE ON THE GROUP OF ISOMORPHISMS OF A GROUP OF ORDER p^m.

By G. A. Miller.

The first part of the following note is devoted to a study of some of the properties of the holomorphisms of a group of order p^m, p being any prime, which correspond to operators whose order is a power of p in the group of isomorphisms. In the second part an abelian subgroup of the group of isomorphisms of any abelian group of order p^m is determined. It is proved that this abelian subgroup is one of a series of conjugate subgroups which have in common the invariant operators of the group of isomorphisms.

1. Let P represent any group of order p^m, p being any prime, and let $P_1, P_2, \ldots . P_m$ represent any series of subgroups of orders $p, p^2, \ldots . p^m$ respectively such that $P_{\alpha-1}$ is contained in P_α, $\alpha = 2, 3 \ldots . m$. The main object of this note is to consider all the holomorphisms of P which can be obtained on condition that every operator of P_α which is not in $P_{\alpha-1}$ corresponds to itself multiplied on the left by some operator of $P_{\alpha-1}$.* It will first be proved that all such holomorphisms of P correspond to operators of order p^λ in the group of isomorphisms (I) of P; and, conversely, that each of the holomorphisms of P which corresponds to an operator of order p^λ in I is of this form.

If t_1, t_2 are any two operators of I which correspond to two such holomorphisms, then must $t_1 t_2$ have the same property. That is, to the totality of the possible holomorphisms for any series of subgroups such as $P_1, P_2, \ldots . P_m$ there corresponds a subgroup (I_1) of I. Let t_3 be any operator of I_1. In the holomorphism which corresponds to t_3 some operator (s) of P corresponds to $s_1 s$, where s_1 is commutative† with t_3. From this it follows that $t_3^{-n} s t_3^n = s_1^n s$, and hence the order of t_3 must be a power of p. Since t_3 is any operator of I_1 it follows that the order of I_1 is a power of p. When P is abelian this result may also be obtained by means of the known formula‡

$$t^{-n} s_\alpha t^n = s_{\alpha+n} s^n_{\alpha+n-1} \cdot \cdot \cdot \cdot \cdot s_{\alpha+n-r}^{\frac{n(n-1)\ldots(n-r+1)}{r!}} \cdot \cdot \cdot \cdot s^n_{\alpha+1} s_\alpha$$

* *Cf.* Burnside, *Theory of Groups of Finite Order*, 1897, p. 249.

† In the substitution group of degree p^m, determined by the two groups P and I. *Cf.* Burnside, *l. c.*, *p.* 227.

‡ *Bulletin of the American Mathematical Society*, vol. 7 (1901), p. 351.

whenever

$$t^{-1}s_\beta t = s_{\beta+1}s_\beta, \qquad \beta = \alpha, \alpha+1, \cdots\cdots \alpha+n-1;$$

for $s_{\alpha+n}$ is the identity if $n > m-1$, and n may be so chosen that each of the exponents

$$n, \cdots\cdots \frac{n(n-1)\cdots\cdots(n-r+1}{r!}, \cdots\cdots n$$

is divisible by any power of p.

Frobenius has proved that in a group (P') of order $p^{m'}$ the total number of subgroups P'' of order $p^{m''}$ $(m'' < m')$ is $\equiv 1 \bmod p$. If P' is an invariant subgroup of our main group P of order p^m, a group P'' is invariant either under P or under one of a set of subgroups P'' conjugate under P. As the total number of these conjugates must be a multiple of p, it follows that the number of subgroups of order $p^{m''}$ which are contained in P' and invariant under P is $\equiv 1 \bmod p$.

We consider now any subgroup $\bar{I}$ of I, the order of $\bar{I}$ being $p^{\bar{n}}$, and prove that it is a subgroup I_1 related in the way explained in the first paragraph to at least one series of subgroups $P_1, P_2, \cdots P_m = P$ of P, in which, furthermore, every subgroup P_α is invariant under P. The group I_1 connected with an arbitrary series of subgroups is such a group $\bar{I}$, and it is connected also with a series of subgroups of the particular character just specified.

The subgroup $\bar{I}$ of I leaves invariant $P = P_m$, and at least one of its invariant subgroups (P_{m-1}) of order p^{m-1}, since its order is a power of p and the number of such subgroups is $\equiv 1 \bmod p$. Similarly it leaves invariant at least one (P_{m-2}) of the subgroups of P_{m-1} which are of order p^{m-2} and invariant under P_m. And so on. Thus the group $\bar{I}$ does leave invariant each one of a series of subgroups $P_1, \ldots P_m$ of the kind specified. But further it leaves it invariant in the way specified in the first paragraph, as one readily proves; for the quotient group $P_{\alpha+1}/P_\alpha$ is of order p and its group of isomorphisms is of order $p-1$, which is prime to the order of $\bar{I}$. Such subgroups as I_1 depend, in general, upon P_1 and also upon the manner of selecting P_2, $P_3, \ldots, P_{m-1}$ after P_1 has been chosen. In particular, when P is cyclic, these subgroups can be chosen in only one way, while they can be chosen in a number of ways depending upon m when P is abelian and of type $(1, 1, 1, \ldots)$. In the latter case the totality of the holomorphisms for one series of subgroups such as $p_1, p_2, \cdots\cdots p_m$ is evidently the same as that for any other series, so that I_1, which is of order $p^{\frac{m(m-1)}{2}}$, has just as many conjugates under I as

there are different ways of selecting such a series; viz. $(p^m-1)(p^{m-1}-1)$ $\cdots\cdots(p-1)\div(p-1)^m$. Each of these conjugates is therefore invariant in a subgroup (I_2) of I, whose order is $p^{\frac{m(m-1)}{2}}(p-1)^m$. Moreover, the quotient group I_2/I_1 is the direct product of m cyclic groups.

In the last example it was observed that, if any of the subgroups P_1, P_2, $\ldots\ldots P_{m-1}$ is replaced by a different one, the corresponding subgroups of I will be conjugate, but not identical with I_1. This is clearly always the case when a holomorphism of P may be obtained by multiplying an operator of P_a by an arbitrary operator of P_{a-1}, $a=2, 3, \ldots\ldots m$. When the last condition is satisfied, let I_2 represent the largest subgroup of I in which I_1 is invariant. We proceed to prove that I_2/I_1 is always a subgroup of the direct product of cyclic groups of order $p-1$.

In all the holomorphisms which correspond to I_2, each of the subgroups $P_1, P_2, \ldots\ldots, P_m$ corresponds to itself, and conversely, if each of these subgroups corresponds to itself in any holomorphism of P, this holomorphism must correspond to some operator of I_2. In all these holomorphisms the operators of P_a/P_{a-1} $(a=2, 3, \ldots m)$ correspond to some power of themselves. Let t_4, t_5 be any two operators of I_2 and consider the holomorphism which corresponds to the commutator of $t_4^{-1}t_5^{-1}t_4t_5$. Since all the operators of P_a/P_{a-1} must correspond to themselves in this holomorphism, it follows from the preceding paragraph that the order of $t_4^{-1}t_5^{-1}t_4t_5$ is a power of p. Hence I_1, which is composed of all the operators of I whose orders are powers of p, must include all the commutators of I. As the quotient group with respect to any invariant subgroup which includes the commutator subgroup is abelian,* I_2/I_1 must be abelian.† Furthermore, since the groups P_a/P_{a-1} are of order p and correspond to themselves in all these holomorphisms, I_2/I_1, *must be included in the direct product of cyclic groups of order* $p-1$.

It may be of interest to observe that a change in the series of subgroups $P_1, P_2, \ldots\ldots P_{m-1}$ does not necessarily affect I_1. For instance, when P is the direct product of two cyclic groups (C_1, C_2) of orders p^{m-1}, p respectively $(m>2)$, its group of isomorphisms (I) is of order $p^m(p-1)^2$.‡ In this case, let C_1 equal P_{m-1}. This determines the series $P_1, P_2, \ldots P_{m-1}$ and the corresponding I_1 is clearly of order p^{m-1}. The subgroup I_1 includes all

* *Quarterly Journal of Mathematics*, vol 28, 1896, p. 267.

† Wendt, *Mathematische Annalen*, vol. 55, 1901, p. 480.

‡ *Cf. Transactions of the American Mathematical Society*, vol. 2, 1901, p. 260.

the operators of I which satisfy the following conditions: the orders are powers of p, and they transform each of the cyclic subgroups of order P^{m-1} in P into itself. When P_{m-1} is replaced by any other cyclic subgroup of the same order, the remaining subgroups of the series $P_1, P_2, \ldots . P_{m-1}$ will not be changed, and the corresponding subgroup of I clearly satisfies the same condition as before, and hence it is identical with I_1.

2. In what follows it will be assumed that P is abelian. If p^{a_1} is the highest order of an operator in P, then it is possible to obtain $p^{a_1-1}(p-1)$ distinct holomorphisms of P by raising each one of its operators to the same power. It is known that these holomorphisms correspond to the $p^{a_1-1}(p-1)$ invariant operators of I.* We proceed to consider an important abelian subgroup of I which includes the characteristic subgroup composed of these invariant operators.

Let $H_1, H_2, \ldots . . H_n$ be any set of independent generating cyclic subgroups of P whose orders are $p^{h_1}, p^{h_2}, \ldots . p^{h_n}$ respectively; and consider any holomorphism of P in which each of these subgroups corresponds to itself. It is clearly possible to establish an arbitrary holomorphism of one of these subgroups with itself without affecting the holomorphism of any one of the other subgroups. Hence it follows that the totality of the holomorphisms of P in which each of these subgroups corresponds to itself must correspond in I to the direct product (A) of n cyclic groups of orders

$$p^{h_1-1}(p-1), \qquad p^{h_2-1}(p-1), \qquad \ldots . . \qquad p^{h_m-1}(p-1)$$

respectively, whenever $p > 2$. When $p = 2$, the subgroup A is the direct product of a group of order 2^n and of type $(1, 1, 1) \ldots . .$ and n cyclic groups of orders $2^{h_1-2}, 2^{h_2-2}, \ldots . . 2^{h_m-2}$ respectively. The only case in which A reduces to the identity is when P is of type $(1, 1, 1 \ldots . .)$ and $p = 2$.

Let $S_1, S_2, \ldots . . S_n$ represent a set of generators of the cyclic subgroups $H_1, H_2, \ldots . . H_n$ respectively, and let $H'_1, H'_2, \ldots . H'_n$ represent a second set of independent generating cyclic subgroups of P. At least one of the latter subgroups (H'_a) is not generated by a single one of the operators of $S_1, S_2, \ldots . . S_n$. A generator of H'_a is therefore of the form $S_a^{a_1} S_\beta^{\beta_1} \ldots \ldots$, where at least two of the exponents $a_1, \beta_1, \ldots .$ differ from zero. As the subgroup A $(p > 2)$ includes some operators which transforms H'_a into itself, multiplied by some operator which is not found in H'_a, it

* *Cf.* the last foot-note.

follows that A *transforms into itself each member of only one of the possible sets of independent generating cyclic subgroups of* P, *whenever* $p > 2$.

From the preceding paragraph it follows that A has as many conjugates under I as there are different combinations of generating subgroups of P, whenever p is odd. In this case I contains no operators that transform A into itself besides those of A and those which transform the totality of the subgroups $H_1, H_2, \ldots. H_n$ into itself, but permute some of them. The latter operators exist only when at least two of the independent generators of P are of the same order. Moreover, P contains no operator besides the identity which is invariant under A.

When $p = 2$, all the operators of order 2 in P are invariant under A, and hence A reduces to the identity when P is of type $(1, 1, 1, \ldots)$, as was observed above from another point of view. Since all the operators of A do not transform into itself any operator of P whose order exceeds 2, they cannot transform each of the subgroups $H'_1, H'_2, \ldots. H'_n$ into itself unless the order of no more than one factor in the product $S_\alpha^{\alpha_1} S_\beta^{\beta_1} \ldots.$ exceeds 2 for every H'_α. This condition is clearly sufficient as well as necessary.

All the conjugates of A have the $p^{\alpha_1 - 1}(p-1)$ invariant operators of I in common for all values of p, since each of these operators transforms every subgroup of P into itself.

Moreover, it is easy to prove that every operator (t) which is found in all the conjugates of A is also included among these invariant operators of I. From the fact that the product $S_1 S_2 \ldots S_n$ may be used as an independent generator of P it follows that

$$t^{-1} S_1 S_2 \ldots. S_n t = (S_1 S_2 \ldots S_n)^\beta \quad \text{and} \quad t^{-1} S_i t = S_i^{\beta_i} \quad i = 1, 2, \ldots, n.$$

Hence

$$(S_1 S_2 \ldots S_n)^\beta = S_1^{\beta_1} S_2^{\beta_2} \ldots S_n^{\beta_n}.$$

We may therefore set $\beta_1 = \beta_2 = \cdots = \beta_n \beta$. Since t transforms each generator of P into its βth power, it also transforms each operator of P into this power; that is, *the* $p^{\alpha_1 - 1}$ $(p-1)$ *invariant operators of* I *are the only ones which are common to all the conjugates of* A *under* I.

STANFORD UNIVERSITY,
JANUARY, 1902.